Daheim ist‘s am schönsten – Anmerkungen zum Urteil in der Rechtssache Schrems

Gastautor 2015-10-13T08:49:33

von LORIN-JOHANNES WAGNER

Mit dem Urteil in der Rs. *Schrems* hat der EuGH einmal mehr gezeigt, dass er es mit der Einhaltung europäischer Datenschutzstandards ernst meint und nicht davor zurückschreckt diese auch vor dem Hintergrund unwägbarer wirtschafts-politischer Konsequenzen aufrecht zu erhalten. Freilich, hält man sich die vorangegangenen Judikate in den Rs. *Digital Rights Ireland* und *Google Spain* vor Augen, konnte, ja, hätte es nicht anders kommen dürfen. Nichtsdestoweniger ist es durchaus bemerkenswert, mit welcher Vehemenz der EuGH die Entscheidung der Kommission über die sog. Safe Harbour Regelung, die die zentrale rechtliche Grundlage für die „freie“ Datenübermittlung in die USA bildete, aus den Angeln hebt. Tatsächlich bleibt mit dem vorliegenden Urteil von Safe Harbour nichts mehr übrig. Über den Anlassfall hinaus untermauert der EuGH in seinem Urteil in der Rs. *Schrems* aber die Wirkmächtigkeit der von ihm determinierten Datenschutzstandards in der Außendimension und betont, wenn auch in der Diskussion bisher kaum beachtet, abermals die zentrale Funktion der Datenschutzkontrollstellen.

Europäischer Datenschutz…weltweit!

Der wesentliche Grundstein für das Urteil *Schrems* liegt dabei in der Feststellung, dass in einem Drittstaat nur dann von einem „angemessenen“ Datenschutzniveau ausgegangen werden kann, wenn das garantierte Niveau „der Sache nach gleichwertig ist“ (Rn. 73). Eine Entscheidung der Kommission, mit der diese die Grundlage für eine „freie“ Datenübermittlung in ein Drittland schafft (vgl. Art. 25 Abs. 6 Datenschutz-RL) – wie etwa jene über Safe Harbour – setzt demnach das Bestehen eines effektiv unionsgleichen Schutzniveaus in dem betreffenden

Drittland voraus. Die Mittel und Wege, wie dieses Schutzniveau erreicht wird, mögen unterschiedlich sein, der Maßstab (sowohl in materieller wie auch rechtsschutztechnischer Hinsicht) ist aber ultimativ durch die DatenschutzRL und die in Art. 7, 8 und 47 GRC verbürgten Rechte vorgegeben. Wenig verwunderlich also, dass der EuGH im Urteil *Schrems* nach diesem Postulat über die „Gleichheit des Datenschutzes“ in einem Drittland auf Kernaspekte seiner „internen“ Datenschutzrechtsprechung zurückgreift, um darzulegen, welchen Anforderungen die rechtlichen Schutzmechanismen in einem Drittstaat genügen müssen (Rn. 91-95) und dies mit der Vorgabe einer strikten und fortwährenden Überprüfung durch die Kommissionverbindet (Rn. 75-78). Für das ohnehin schwerfällige System der einseitigen Anerkennung eines angemessenen Datenschutzniveaus durch die Kommission nach Art. 25 Abs. 6 Datenschutz-RL stellt sich angesichts dieser Vorgaben freilich insgesamt die Sinnfrage: Ist ein System, dass auf der Grundalge einseitiger Feststellungen und Zuschreibungen von Datenschutzstandards operiert in einer globalisierten und vernetzten Welt tatsächlich funktionsfähig? (Siehe hierzu auch *Kuner auf dem Verfassungsblog*)

Ungeachtet dieser Systemfrage fügt sich das Urteil aber nahtlos in die – wenn man so will – „globale“ Datenschutzrechtsprechungslinie des EuGH ein, die auf der Prämisse fußt, dass der in der EU vorgegebenen Datenschutzstandard, unabhängig davon, wo „europäische Daten“ verarbeitet werden, zu gelten hat. Das vorliegende Urteil rundet insoweit den in der Rs. *Google Spain* vorgezeichneten Ansatz „extraterritorialer Erstreckung“ des europäischen Datenschutzrechts ab und exemplifiziert das unverkennbar „expansive“ (Grund-)Rechtsverständnis des EuGH – zumindest für den Bereich des Datenschutzes. Die Expansionsmodi in *Schrems* (mittelbar) und *Google Spain* (unmittelbare Erstreckung auf außerhalb der Union ansässige für die Datenverarbeitung Verantwortliche) sind zwar unterschiedlich, das dahinter liegende Motiv ist bei beiden aber dasselbe: Die Wahrung des Datenschutzes in der Union ist letztlich davon abhängig, dass Datenschutzstandards nicht durch den Datenexport und die Verarbeitung „europäischer Daten“ im Ausland unterlaufen werden können.

Ob sich dieser expansive Datenschutzanspruch europäischen Zuschnitts angesichts divergierender Vorstellungen über den Schutz der Privatsphäre in der Praxis aufrechterhalten lässt, ist freilich eine andere Frage. Wobei dies nicht zuletzt davon abhängig sein wird, ob es gelingt die konfligierenden Ansätze durch die Normierung gemeinsamer internationaler Datenschutzstandards einzuebnen. (siehe hierzu allgemein und vertiefend *Wagner, Der Datenschutz in der Europäischen Union*). Vor dem Hintergrund der bestehenden Judikaturlinie ist freilich nicht schwer zu erahnen, dass der EuGH wohl aber auch bei der Prüfung internationaler Übereinkommen, die den Austausch und/oder Schutz europäischer Daten betreffen, an seinem strengen Datenschutzmaßstäben festhalten wird. Abseits der hierdurch vorgezeichneten Probleme für bestehende und viel kritisierte Übereinkommen, wie insbes. die Abkommen über die Übermittlung von Fluggastdaten und SWIFT-Daten, tun die Institutionen damit wohl gut daran, sich bei der Verhandlung neuer Übereinkommen, wie etwa dem EU-USA Data Protection Umbrella Agreement, die Datenschutzrechtsprechung des EuGH im Detail zu vergegenwärtigen.

Dass die inhaltlichen Ausführungen zu den Anforderungen an die Gleichwertigkeit des Schutzniveaus im Urteil *Schrems* eigentlich aber nur Randbemerkungen bleiben, liegt an der grds. verfehlten Konstruktion von Safe Harbour und der hierauf aufbauenden Kommissionsentscheidung: Safe Harbour beruht nämlich auf einem Mechanismus der Selbstzertifizierung von in den USA niedergelassenen Organisationen, ohne dass in den USA tatsächlich ein rechtlicher Rahmen bestünde, um die Einhaltung der durch die Selbstzertifizierung anerkannten Datenschutzstandards sicherzustellen (Rn. 81). Da die Kommission in ihrer Entscheidung über die Angemessenheit von Safe Harbour weder dies berücksichtigt, noch Feststellungen zur „Angemessenheit" des rechtlichen Rahmens bei einer weitergehenden Verarbeitung der übermittelten Daten durch staatliche Behörden trifft (Rn. 81 ff), kommt der EuGH unversehens zum Ergebnis, dass die Kommission in ihrer Entscheidung gar „nicht festgestellt [hat], dass die Vereinigten Staaten von Amerika aufgrund ihrer innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein angemessenes Schutzniveau ‚gewährleisten'" (Rn. 97). Die Entscheidung der Kommission genügt damit schon aus „formaler" Sicht nicht den Anforderungen an eine Entscheidung über die Angemessenheit des Datenschutzniveaus in einem Drittland (Rn. 96), ohne dass der EuGH tatsächlich in eine inhaltliche Prüfung der Grundsätze des „sicheren Hafens" einsteigen muss (Rn. 98).

Dass sich der EuGH nichtsdestotrotz mit den Bedingungen für die Feststellung eines angemessenen Datenschutzniveaus auseinandersetzt, liegt wohl nicht zuletzt darin begründet, dass mit dem Wegfall von Safe Harbour nunmehr die Mitgliedstaaten gefordert sind, im Vorfeld geplanter Datenübermittlungen in die USA, über die Angemessenheit des Datenschutzniveaus zu befinden (vgl. Art. 25 Abs. 1 Datenschutz-RL). Die Ausführungen des EuGH lassen sich insoweit als allgemeine Konkretisierung des Prüfrasters für die Beurteilung der Angemessenheit des Datenschutzniveaus in Drittländern lesen. Zugleich legen zugleich sie aber offen, dass der EuGH den uneingeschränkten Zugriff staatlicher Behörden auf übermittelte Daten – und deren Inhalt – sowie das gänzliche Fehlen wirksamer Rechtsschutzinstrumente in den USA für grds. unvereinbar mit dem (Wesen des [vgl. insbes. Rn. 94 und 95]) europäischen Datenschutzverständnis(ses) erachtet. (Zur problematischen impliziten Erstreckung des Anwendungsbereichs des europäischen Datenschutzrechts auch auf den Bereich der nationalen Sicherheit siehe den Beitrag von Peters)

Kommission vs. Nationale Datenschutzkontrollstellen – Unabhängigkeit und über-subjektiver Schutzanspruch in der vertikalen Dimension

Das vorliegende Urteil enthält auch neben der angesprochenen „globalen Dimension" Bemerkenswertes: So untermauert der EuGH mit *Schrems* nämlich abermals die zentrale Bedeutung nationaler Datenschutzkontrollstellen für die Wahrung des (Grund-)Rechts auf Datenschutz (siehe Art. 8 Abs. 3 GRC). Im Unterschied zu vorangegangenen Urteilen (vgl. Rs. *Kommission/Österreich* sowie *Kommission/Deutschland*) stärkt der EuGH im Urteil *Schrems* die Unabhängigkeit der nationalen Kontrollstellen aber nicht gegenüber den Mitgliedstaaten,

sondern emanzipiert diese gegenüber der Kommission: Die Befugnis nationaler Kontrollstellen, Beschwerden gegen Datenübermittlungen in ein „sicheres“ Drittland zu prüfen und gegebenenfalls Maßnahmen gegen die Übermittlung zu treffen (vgl. Art. 28 Datenschutz-RL), besteht nämlich unabhängig von einer Entscheidung der Kommission über ein „angemessenes“ Datenschutzniveau in dem betreffenden Drittland (siehe insbes. Rn. 53 und 58) – folgerichtig können diese Befugnisse auch nicht durch eine Entscheidung der Kommission eingeschränkt werden (Rn. 103). Der EuGH geht hier noch einen Schritt weiter und verlangt, dass dort, wo nationale Kontrollstellen begründete Zweifel an der Angemessenheit des Datenschutzniveaus und damit (implizit) an der Entscheidung der Kommission hegen, diesen eine Klagemöglichkeit nach nationalem Recht offenstehen muss, um inzident die Gültigkeit der Kommissionsentscheidung in Frage zu stellen (Rn. 65). Dieses Klagerecht ist zwar zugegebenermaßen etwas ungelenk, aber nur konsequent, wenn man sich die „über-subjektive“ Schutzfunktion nationaler Kontrollstellen vor Augen hält und nationale Kontrollstellen nicht selbst als Gerichte i.S.v. Art. 267 AEUV ansehen wollte – was im Übrigen angesichts ihrer gerichtsähnlichen Unabhängigkeit nicht unumstritten war (siehe hierzu auch die zurückgezogene Vorlagefrage der österreichischen Datenschutzbehörde).

Aus dieser erweiterten Rechtsschutzfunktion ergibt sich allerdings die Folgefrage, ob nunmehr für nationale Kontrollstellen im Falle von begründeten Zweifeln an der durch die Kommission attestierten Angemessenheit des Datenschutzniveaus in einem Drittland – in Anlehnung an die *Foto Frost*–Rechtsprechung – eine Klagepflicht vor nationalen Gerichten besteht? Das Urteil ist in dieser Hinsicht zwar erratisch, man wird wohl aber in Anbetracht der Funktion nationaler Kontrollstellen sowie aus Gründen der Rechtssicherheit und der Wahrung der einheitlichen Anwendung des Unionsrechts annehmen müssen, dass nationale Kontrollstellen, wenn sie, wegen begründeter Zweifel an der Angemessenheit des Datenschutzniveaus in einem „sicheren“ Drittland, Maßnahmen gegen eine konkrete Datenübermittlung ergreifen, auch eine Verpflichtung trifft, die Gültigkeit der Kommissionsentscheidung (inzident) zu bestreiten. Die Befugnis, entsprechende Maßnahmen zu erlassen, ist dabei allerdings nicht an die Erhebung einer solchen Klage gebunden – diese besteht vielmehr, wie der EuGH betont, als unabhängiges Recht der nationalen Kontrollstellen (vgl. hierzu auch die Schlussanträge von GA *Bot*, Rn. 81 und 118) – und unterliegt damit auch nicht den strengen Vorrausetzungen des einstweiligen (gerichtlichen) Rechtsschutzes gegen Unionsrechtsakte (vgl. *Zuckerfabrik Süderdithmarschen*).

Das vorliegende Urteil fügt sich damit als weiterer Baustein in die Bewehrung der Unabhängigkeit der Datenschutzkontrollstellen – „zur Abwechslung“ diesmal allerdings in der vertikalen Dimension –und verdeutlicht exemplarisch, dass die grundrechtliche Funktion der (nationalen) Datenschutzkontrollstellen mit einem über-subjektiven Schutzanspruch einhergeht. Das Urteil darf und muss insoweit wohl auch als Vorgabe für die zukünftige Ausgestaltung des Verhältnisses von Kommission und nationalen Datenschutzkontrollstellen sowie deren notwendige Befugnisse in einem vernetzten europäischen Verwaltungsverbund gelesen werden (vgl. hierzu insgesamt auch die Vorschläge für eine Datenschutzreform).